OIPE IAP86 NOV 05 2007 PATENT & TRADEMARK OFFICE

PTO/SB/08A (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Virgil A. Herring
Attorney Docket Number	44424162-8724

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/VH/	2V	US- 4202051	05-06-1980	Davida	
/VH/	2W	US- 4905176	02-27-1997	Schulz	
/VH/	2X	US- 5557346	09-17-1996	Lipner	
/VH/	2Y	US- 5623548	04-22-1997	Akiyama	
/VH/	2Z	US- 5625692	04-29-1997	Herzberg	
/VH/	3A	US- 5625695	04-29-1997	M'Hraihi	
/VH/	3B	US- 5727062	03-10-1998	Ritter	
/VH/	3C	US- 5745577	04-28-1998	Leech	
/VH/	3D	US- 5778069	07-07-1998	Thomlinson	
/VH/	3E	US- 5870478	02-09-1999	Kawamura	
/VH/	3F	US- 5998978	12-07-1999	Connell	
/VH/	3G	US- 6028454	02-22-2000	Elmasry	
/VH/	3H	US- 6345359	02-05-2002	Bianco	
/VH/	3I	US- 6748410	06-08-2004	Gressel	
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Virgil Herring/ (11/18/2007)	Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete If Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Virgil A. Herring
Attorney Docket Number	44424162-8724

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/VH/	3J	VISA INTERNATIONAL SERVICE ASSOCIATION'S PRELIMINARY INVALIDITY CONTENTIONS, FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division, June 2, 2005	
/VH/	3K	KUHN and ANDERSON, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations." Proceedings of the Second International Workshop on Information Hiding, Portland, Oregon, April 1998, pages 124-142.	
/VH/	3L	MENEZES, et al., "CRC Handbook of Applied Cryptography", Boca Raton, Florida: CRC Press LLC, 1996, pages 591-634.	
/VH/	3M	VISA INTERNATIONAL SERVICE ASSOCIATION'S FINAL INVALIDITY CONTENTIONS FOR U.S. PATENT NO. 6,278,783 FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division, June 28, 2007	
/VH/	3N	ALON, et al., "Efficient Dynamic-Resharing 'Verifiable Secret Sharing' Against Mobile Adversary", Mar. 25, 1995	
/VH/	3O	CHARNES, et al., "Comments on Soviet Encryption Algorithm", Springer-Verlag, 1998	
/VH/	3P	MAURER, UELI M., "A Provably-Secure Strongly-Randomized Cipher", Springer-Verlag, 1998	
/VH/	3Q	MEIJER and AKI, "Digital Signature Schemes", May 1982, Extended summary of paper prsented at CRYPTO 81, Santa Barbara, CA, August 1981	
/VH/	3R	SHAMIR, ADI, "How to Share a Secret", Communications of the ACM November, 1979, Volume 22, Number 11	
/VH/	3S	VISA INTERNATIONAL SERVICE ASSOCIATION'S FINAL INVALIDITY CONTENTIONS FOR U.S. PATENT NO. 6,298,442 FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division, July 16, 2007	

Examiner Signature	/Virgil Herring/ (11/18/2007)	Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Virgil A. Herring
Attorney Docket Number	44424162-8724

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/VH/	3T	BRICKELL, et al., "Fast Exponentiation with Precomputation (Extended Abstract)", Springer-Verlag, 1998	
/VH/	3U	DE ROOIJ, PETER, "Efficient Exponentiation using Precomputation and Vector Addition Chains", Springer-Verlag, 1998, possibly a reprint from Advances in Cryptology, EUROCRYPT '94, 1994	
/VH/	3V	DIMITROV, et al., "An Algorithm for Modular Exponentiation", Information Processing Letters, Volume 66, Issue 3, pp.155-159, May 15, 1998	
/VH/	3W	DIMITROV, et al., "Two Algorithms for Modular Exponentiation Using Nonstandard Arithmetics", IEICE Trans. Fundamentals, Vol. E78-A, No. 1, January 1995	
/VH/	3X	GOLLMAN, et al., "Redundant Integer Representations and Fast Exponentiation", Designs, Codes and Cryptography, 7, 135-151, Kluwer Academic Publishers, Boston, MA, 1996	
/VH/	3Y	HONG, et al., "New Modular Multiplication Algorithms for Fast Modular Exponentiation", Springer-Verlag, 1998, from Advances in Cryptology, EUROCRYPT '96, 1996	
/VH/	3Z	JEDWAB and MITCHELL, "Minimum Weight Modified Signed-Digit Represenations and Fast Exponentiation", Electronics Letters, V. 25, No. 17, Aug. 17, 1989.	
/VH/	4A	KOÇ, ÇETIN K., "High-Radix and Bit Recoding Techniques for Modular Exponentiation", Intern. J. Computer Math, v. 40 pp. 139-156, 1991, Gordon and Breach Science Publishers, S.A. (UK)	
/VH/	4B	EĞECIOĞLU and KOÇ, "Exponentiation using Canonical Recoding," Theoretical Computer Science 129, pp. 407-417, Elsevier, 1994	
/VH/	4C	KOÇ, ÇETIN K., "High-Speed RSA Implementation", RSA Laboratories, November 1994	

Examiner Signature	/Virgil Herring/ (11/18/2007)	Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/08B (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 4

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Art Unit	2132
Examiner Name	Virgil A. Herring
Attorney Docket Number	44424162-8724

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/VH/	4D	LIM and LEE, "More Flexible Exponentiation with Precomputation", Advances in Cryptology, Springer-Verlag, 1998,possibly from CRYPTO '94, August 1994	

Examiner Signature	/Virgil Herring/ (11/18/2007)	Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.